



# UNITED STATES PATENT AND TRADEMARK OFFICE

*mn*

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,935	12/10/2003	Daniel Alan Brokenshire	AUS920030716US1	8691

50170 7590 06/28/2007

IBM CORP. (WIP)

c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.

P.O. BOX 832745

RICHARDSON, TX 75083

EXAMINER

LASHLEY, LAUREL L

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

06/28/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

Application No.

10/733,935

Applicant(s)

BROKENSHERE ET AL.

Examiner

Laurel Lashley

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 10 December 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1 – 16 are pending and have been examined.

#### ***Specification***

2. The specification is objected to because of the following informalities:

- Abbreviation must be spelled out when used for the first time (e.g. CBC on page 2)
- CBM-MAC acronym is inconsistent with its noted spelled out version (see page 6).

Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 – 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 1 recites the limitations "sending... to a/the receiver;" and "sending....to a target;". The Examiner has interpreted "the receiver" and "a target" to be one and the same, clarification is requested.

5. Claims 1, 15 and 16 recite the limitation "the received message" and "the received publicly known constants". There is insufficient antecedent basis for these limitations in the claims.

Claim 12 recites the limitation "the secret key" and "the security function". There is insufficient antecedent basis for these limitations in the claims.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2132

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1 – 4, 7 – 16 are rejected under 35 U.S.C. 102(b) as being anticipated by Connery et al in US Patent No. 6311276 (hereinafter US '276).

7. For claims 1, and similar claims 7, 15, and 16, US '276:

A method for authenticating a message, comprising: (see Abstract: message authentication)

performing a security function upon the message; (see Abstract: security feature added to packet)

sending the message to a receiver; (see column 2, lines 45 – 47: security logic receives message from source)

sending the output of the security function to a target; (see column 2, lines 25 – 26)

sending at least one publicly known constant to the receiver; (see column 2, lines 35 – 39: timestamp)

authenticating the received message as a function of at least a shared key, the received publicly known constants, the security function, the received message, and the output of the security function (see Abstract; column 2, lines 26 – 45; column 3, lines 34 – 38, 51 – 61: shared secret value, timestamp, security feature, hash function).

For claim 2 and similar claim 9, US '276 discloses:

The method of claim 1, wherein the security function comprises a hash function. (see column 2, lines 31 – 33: hash function)

For claim 3, US '276 discloses:

The method of claim 1, wherein the authentication comprises a determination that the message is authentic. (see Abstract: accepted message must pass authentication)

For claim 4, US '276 discloses:

The method of claim 1, wherein the authentication comprises a determination that the message is not authentic. (see Abstract: discarded message failed authentication)

For claim 8, US '276 discloses:

The system of claim 7, wherein the source node comprises a computer. (see Figure 2, end station)

For claim 10, US '276 discloses:

The system of claim 7, further comprising an unsecured medium coupled between an output of the source node and an input of the target node. (see Figure 1, item 20)

For claim 11, US '276 discloses:

The system of claim 7, wherein the source node is further configured to generate a message authentication code (MAC). (see column 2, lines 25 – 26: message from source includes MAC)

For claim 12, US '276 discloses:

The system of claim 7, wherein the MAC is a function of at least a message, the secret key, the security function and the publicly known constants. (see column 2, lines 28 – 39: MAC comprising message digest of message, secret value, timestamp...)

For claim 13, US '276 discloses:

The system of claim 7, wherein the target node is further configured to receive a message authentication code (MAC). (see column 2, lines 25 – 26: received message includes MAC)

For claim 14, US '276 discloses:

The system of claim 13, wherein the target node is further configured to employ the MAC to authenticate a received message from the source node. (see column 3, lines 34 – 38)

***Claim Rejections - 35 USC § 103***

Art Unit: 2132

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Connery et al. further in view of Sibert in US Patent No. 6832316 (hereinafter US '316).

9. For claim 5 and 6, US '276 discloses a security function (see Abstract: security feature) but does not expressly disclose the security function comprising an encryption function and decryption function respectively.

Sibert, however in US '316, discloses a security function comprising an encryption function and decryption function (see Abstract: integrating message authentication with encryption and decryption).

Connery et al. and Sibert are analogous art because they are from the same problem solving areas (message authentication). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the security feature added to a message of Connery et al. such that it would incorporate an encryption and decryption function as in Sibert. The motivation for doing so would have been to improve the security of the message.

### ***Conclusion***

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley  
Examiner  
Art Unit 2132

21 June 2007  
LLL

*[Handwritten signature]*  
Benjamin S. Lashley  
Examiner Art 2132